Bitcoin as Decentralized Money: Current Landscape and Future Challenges of 2nd Layer

Kenichi Kurimoto, Hiroshi Ueno, and Hitomi Moriyama

Abstract. The future direction of Bitcoin is challenging to discuss due to its decentralized nature and the absence of a clear definition of its future goals, which stems from this decentralized nature. Furthermore, its increasing connection to external society is rapidly increasing the number of involved parties and the possibility of external influence. This paper aims to mitigate this difficulty by providing various classifications and definitions for Bitcoin technologies, focusing on the critical criterion of decentralization. We define effective decentralization by incorporating the criterion of the practical difficulty for regulatory authorities to control the system, while also accounting for the influence over the direction of development, and the resulting impact on future goals. We analyze the Lightning Network (LN) as a representative Bitcoin 2nd Layer technology, detailing the trade-offs between the highly decentralized but complex Pure LN and the user-friendly but centralized Custodial LN and LSP LN. By comparing the LN with Ethereum Rollups, we highlight the architectural differences, particularly the challenge of achieving non-custodial self-withdrawal within a rollup-style architecture on Bitcoin's constrained script environment, versus the relative ease on Ethereum Rollups. While the Pure LN largely preserves the properties of the 1st Layer, its difficult User Experience has led to high usage of custodial solutions. In conclusion, this paper argues that prioritizing the decentralization of the money itself is essential for Bitcoin's success as Decentralized Money. At the same time, given the unpredictability of future regulations, it is vital for the ecosystem to pursue diverse initiatives and applications across various 2nd Layer architectures.

Keywords: Bitcoin 2nd Layer · Decentralization · regulation.

1 Introduction

Discussions surrounding the future of Bitcoin are inherently difficult. This challenge stems from the fact that Bitcoin is a decentralized system, meaning there is no clear definition of "what Bitcoin is supposed to achieve in the future." The Bitcoin algorithm, invented by Satoshi Nakamoto [1], is an open, asynchronous system with free entry and exit, which effectively enables consensus primarily through a majority of hash power.Furthermore, Bitcoin upgrades are implemented through a specialized form of majority consensus. Bitcoin is like a language; while a common language exists, various new colloquialisms emerge, and those that gain broad adoption become part of the common language. Due

to these characteristics, while technical elements are clearly documented, it is difficult to assert or discuss the future direction and governance of Bitcoin.

Moreover, Bitcoin began with individuals who agreed with the system at the time participating in its operation and improvement, engaging in sending and receiving Bitcoin. However, with the launch of ETFs and other developments, its connection to the general external society is rapidly increasing, and the number of people involved is growing. This situation raises the possibility of affecting Bitcoin itself. Many technologies categorized as "2nd Layer" within the Bitcoin ecosystem specifically aim to become the foundation for applications serving the general public.

In this paper, we will:

1. Provide various classifications and definitions to mitigate the difficulty of discussion as much as possible, and explain them.
2. Describe the advantages and disadvantages of the Lightning Network [2] as a representative Bitcoin 2nd Layer technology. We will also examine Ethereum Rollup as a representative 2nd Layer technology for smart contract chains and compare it with the LN.
3. Explain the current situation surrounding the Bitcoin 2nd Layer and offer the author's personal views on its future.

Section 1, in particular, is technically demanding but is given a large proportion of this paper, as the author is confident it will be meaningful.

2 System Model and Definitions

As mentioned in the Introduction, because the direction of Bitcoin's upgrades is decided by a special majority consensus, it is difficult to define "what Bitcoin is supposed to achieve in the future." This is, in itself, the most crucial topic for debate, but it is outside the scope of this paper. We will proceed with the premise that "Bitcoin is an endeavor aimed at creating and disseminating Decentralized Money that anyone can hold and send by their own free will."

Other assumptions are also possible, such as "Bitcoin is a new asset but not money; therefore, P2P transfers should be regulated," or "Bitcoin is both an asset and money, and it should serve as the foundation for decentralized financial applications." In such cases, the resulting arguments would likely take different forms.

2.1 Decentralization

Decentralization is defined here as a state where a system, formed by a large collection of independent individuals and entities with the freedom to join or leave, operates and improves through decision-making based on some form of majority consensus. To avoid the ambiguity of these terms, some suggest a definition stating that "no specific entity (individual or corporation) has control over the decision-making process." However, the author contends that there is a distinct

difference between these two perspectives. The words "large collection" and "independent" used here represent a gradient; however, they are crucial because a significant difference arises from the standard: "Is it practically controllable or difficult to control by regulatory authorities?" Even if a specific entity cannot control the decision-making power, if the system were run by, for example, five giant corporations headquartered in advanced countries with no major political conflicts, regulatory control through business laws is imaginable and not difficult. Conversely, if hundreds of individuals across dozens of countries are responsible for operation and improvement, regulatory control would be extremely difficult. While this criterion itself is not precise, it is clearly one that should be consciously considered.

The next important point is that, currently, Decentralization cannot be achieved by technology alone. Satoshi's invention made it possible to achieve a level of decentralization that was previously impossible. However, if, for example, more than 51 percent of the hash power, which appears anonymously distributed, is actually owned by the same person, and more than 51 percent of the full node instances used for sending and receiving are also operated by the same person, then decentralization is not achieved. In other words, current Public chain technology is merely "technology that enables Decentralization under certain usage conditions." Nevertheless, maintaining, improving, and expanding this "technology that enables Decentralization under certain usage conditions" is a highly difficult and significant effort. Fig. 1 shows this structure.

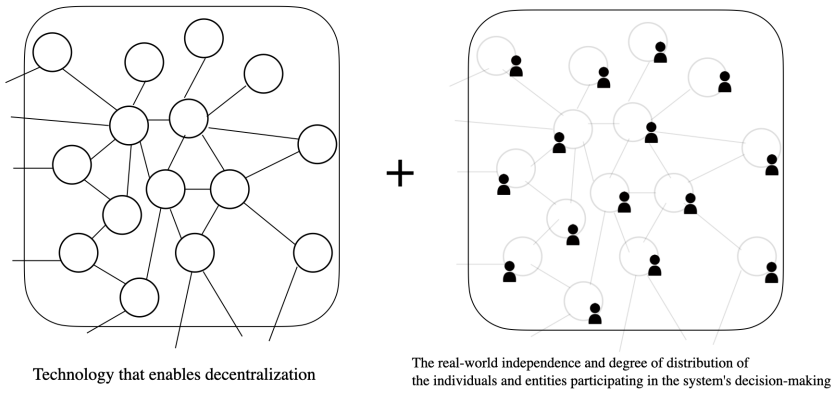


Fig. 1. Two Factors to Achieve Decentralization

While we use the ambiguous phrase "some form of majority consensus," in Bitcoin, the amount of hash power held primarily exerts significant influence

on decision-making. Since miners with substantial hash power are essentially corporations, their shareholders indirectly hold influence. Furthermore, if mining pools create block templates, the parts dependent on the block template are influenced by the mining pools (this area is currently undergoing technical changes). Regarding technical upgrades, users running full nodes have, at times, held influence [3].

Since upgrade proposals are made in source code, individuals capable of making proposals are necessary, but the number of people with the technical knowledge and implementation skill to propose actual Bitcoin upgrades is very small. Therefore, developers also wield significant influence over decision-making.

Additionally, although not currently present in Bitcoin, if a massive stablecoin is used like a standard currency in other smart contract chains, the issuing company is expected to have a very strong voice in system upgrades.

This complex interplay of majority influence changes according to the technical status at any given time.

2.2 External Influences on the Technical System

In the previous section, we defined a criterion for Decentralization based on whether regulation can exert influence. Here, we consider the actual methods of regulatory influence. Regulations primarily apply to the individuals and corporations participating in the network, rather than the network itself. In most countries, individuals are protected from government infringement of their rights by the constitution. Regulating individuals involves a trade-off discussion between the government's right to maintain social stability and the individual's rights, such as freedom of speech and property rights. In contrast, for profit-making corporations, regulations are applied through business laws, placing the state, which has regulatory agencies, in a position where it can more easily impose regulations. Current regulations concerning Bitcoin-related activities are primarily implemented through business laws. Thus, the criterion "Is it practically controllable or difficult to control by regulatory authorities?" is a gradient benchmark, where a decentralized network involving the largest possible number of individuals and companies across the largest possible number of countries in its operation and improvement represents one end of the spectrum. (Even if it is unclear whether regulatory authorities actually use such criteria as a reference for imposing regulations, this will influence what architecture development resources are committed to, given the uncertainty of future regulations).

2.3 AML and Crypto Assets

This paper assumes that "Bitcoin is an endeavor aimed at creating and disseminating Decentralized Money that anyone can hold and send by their own free will". The most crucial topic, which is outside the scope of this paper, is finding the right balance between this goal and Anti-Money Laundering (AML) regulations. In section 2.1, we introduced the criterion of "Is it practically controllable or difficult to control by regulatory authorities?" There are also documents

that state that if P2P transactions become numerous in the future, regulations on them will need to be considered—otherwise the current regulations would lose their meaning—and therefore monitoring is necessary; however, it remains unclear at present who, when, by what means, and through what stages such regulations would be introduced. [4]

It is imaginable that in a sufficiently decentralized system, regulatory control would be challenging. Conversely, providing a user experience (UX) that is freely usable by a large number of users while achieving sufficient decentralization is also highly difficult. In this context, some argue that since sufficient decentralization is highly difficult, we should settle for a certain degree of achievement and aim to clear the necessary conditions through increased encryption. However, maintaining even a partially achieved level of decentralization is also difficult, so this paper does not consider the combination of decentralization and End-to-End (E2E) encryption.

3 2nd Layer Technologies: Lightning Network and Comparison with Other Technologies

3.1 Definition and Scope of Second-Layer Technologies

The definition of 2nd Layer technology itself is not clear. In Bitcoin, the term 2nd Layer technology became commonly used starting with the Lightning Network. Initially, many people used the term to mean technologies built on a higher layer to extend Bitcoin, providing speed and scalability while keeping the properties of the 1st layer as much as possible. Since the Lightning Network enables real-time, small-scale payments, aligning with the expectation that Bitcoin would be used for payments, the motivation for its development was clear. The term has since evolved to generally refer to protocols created at the interface between the 1st Layer protocol and real-world services.

The development of 2nd Layer technologies is also remarkable in smart contract chains other than Bitcoin. They are often broadly classified into Payment channel, Sidechain, and Rollup types, but given the rapid progress in this field, there is no clear and fixed classification. Here, we will compare the Lightning Network, a representative Bitcoin 2nd Layer technology, with Rollup, a representative Ethereum 2nd Layer technology.

3.2 Decentralization and Trust Analysis of the Lightning Network

The Lightning Network is a network composed of numerous payment channels between two participants. Unlike the Bitcoin 1st Layer, the protocol specification (BOLT) itself is stipulated by the community. The protocols described in BOLT are P2P, but in reality, many users use custodial Lightning Networks. Here, we will explain

a) the Pure Lightning Network described in BOLT
b) the Custodial Lightning Network

c) the Mobile Lightning Network connected via an LSP (Lightning Service Provider), which can be seen as an intermediate solution.

Fig. 2 shows overview of these three architecture. Intermediate solutions like c) are being developed for many Public chains, and various proposals and developments are ongoing for Bitcoin as well.

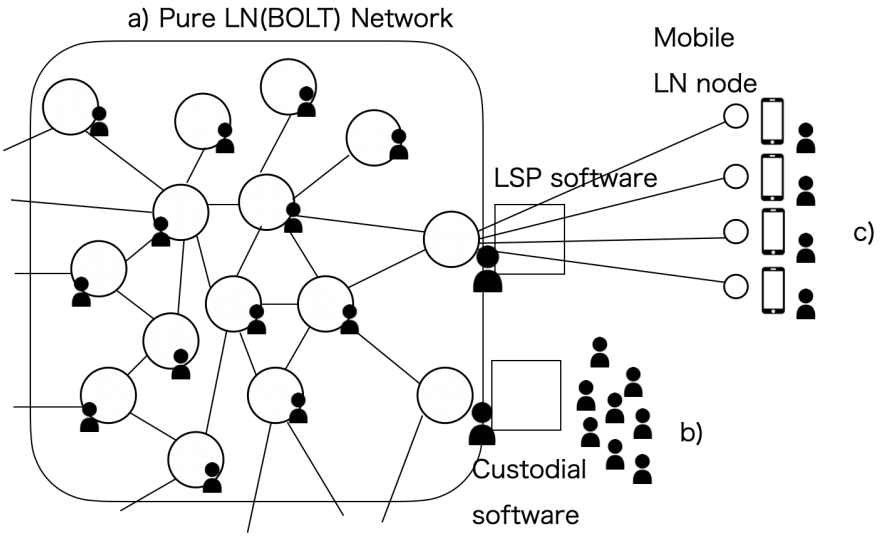


Fig. 2. Classification of the Lightning Network (LN) by Trust Model

a) Pure Lightning Network as defined in BOLT [4]: This network is formed by individuals and entities running bitcoind and operating Lightning Network software. One of its significant distinguishing features is that the participants themselves constitute the components of the P2P network, thereby permitting any individual to engage in permissionless sending and receiving of funds through the Lightning Network with any other party.

Network participants establish payment channels with several other participants and advertise the existence of their node. By collecting this advertised information, network participants can construct a map of the current network structure, determine the route for their own transactions, and relay transactions for other participants. There are also nodes that do not advertise themselves and connect to advertised, relaying nodes. Since the state of a payment channel can be challenged by deploying the past state to the 1st layer, network participants must monitor the 1st Layer. Pure Lightning Network nodes rely on running bitcoind for this monitoring.

Lightning Network participants can maintain Decentralization and conduct transactions in a Trustless manner while preserving the properties of the 1st Layer. The network's overall transaction processing speed (TPS) depends on the composition of relayed transactions but is significantly higher than the 1st Layer, and actual transaction processing is usually completed in real-time. On the other hand, there is an upper limit to the number of participants who can join the Pure Lightning Network. Participation requires a channel-opening transaction to be confirmed on the Bitcoin 1st Layer, and the block size limit of the 1st layer restricts the number of new participants every 10 minutes. Furthermore, the advertisement data itself increases on the network as the number of nodes grows. The number of non-advertising nodes that an advertising node can support is limited by its CPU performance, and it is unclear how large the network can grow in terms of node count.

In any case, it is likely difficult for the entire human population to participate in this network with current technology. Also, to participate in this network, one must monitor the 1st Layer at least once within a certain period, be online to receive funds, and manage the channel balance oneself. These hurdles in current technology likely restrict the number of participants to a level below the network's theoretical maximum.

b) Custodial Lightning Network: Given the difficulties in network participation described above, this service allows users to deposit Bitcoin with a proxy who handles network participation and provides a simpler UX. Users of this service naturally sacrifice the properties of Decentralization and Trustlessness inherent to the Bitcoin 1st Layer. However, as noted earlier, user adoption is a crucial factor in the 2nd Layer, indicating that there are people who prioritize using Bitcoin for transactions and payments, even if they do not prioritize Decentralization or Trustlessness. Considering that many people also hold their Bitcoin custodially on the 1st Layer, this phenomenon is rational.

As custodial operations are regulated in numerous jurisdictions, users of custodial Lightning Network services do not have the ability to send or receive funds to and from arbitrary parties without restrictions.

c) Mobile Wallet using an LSP (Lightning Service Provider): This represents an intermediate solution. The mobile wallet vendor operates a Lightning Network node, and the mobile wallet acts as a leaf node, constantly connected with an open channel to that vendor's node. In this configuration, to prevent the wallet vendor from stealing funds, the mobile wallet must be powered on and monitor the 1st Layer periodically. With this periodic monitoring in place, this form maintains the property that the individual can manage their funds (as there is no possibility of the wallet vendor stealing them), but it does not maintain the property of Decentralization, as sending and receiving depends on the wallet vendor. Efforts also exist to enable connection to various LSPs.

Thus, while the Lightning Network itself as specified in BOLT is designed to maintain the properties of the Bitcoin 1st Layer as much as possible, in practice, various types of 'Lightning Networks' have been constructed over it. Table 1

shows the characteristic comparison of Lightning Network, Custodial LN, and LSP LN.

Table 1. The characteristics of the Lightning Network and its extension technologies

	decentralization	non-custodial	Trustless Tx
Pure LN	Yes	Yes	Yes
Custodial LN	No	No	No
LSP LN	No	Yes	No

3.3 Comparative Analysis with Ethereum Rollups

Here, we will examine Rollup, a representative 2nd Layer technology for Ethereum, and compare it with the Lightning Network. Rollup is a blockchain structure where only the execution layer is moved to a separate blockchain bridged from the Ethereum 1st Layer, while data availability and consensus are entrusted to the Ethereum 1st Layer.

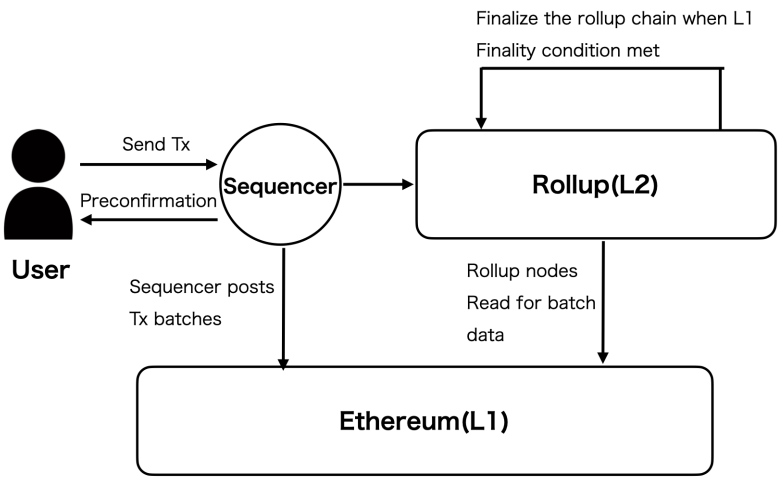


Fig. 3. Rollup architecture from The Practical Guide to Ethereum Rollups: Hackernoon [6]

Fig. 3 shows overview of Rollup architecture [6]. The Sequencer selects user transactions to be included in a block, compresses and batches them through various methods, and subsequently commits the data to the Layer 1. Once written to L1, the transaction is finalized and executed by the execution layer on

Rollup chain. The Sequencer also notifies the user upon selecting the transaction set, allowing the user to receive a provisional confirmation earlier.

There are various types of Sequencer architectures, including those run by a single entity, those run by multiple entities (e.g., round-robin), and those run by multiple entities with Byzantine fault tolerance. Research is also underway on L1 validators taking on the role of the Sequencer. If the Sequencer is a single entity, it has completely abandoned the characteristic of Decentralization, prioritizing the fast sending and receiving of Eth or tokens, and the fast execution of a large volume of smart contracts. Similarly, in a multi-entity format without Byzantine fault tolerance, like round-robin, a significant degree of Decentralization can be considered abandoned.

Regarding the Byzantine Fault Tolerant (BFT) format, there is a gradient based on both the number of participating entities and their independence. Still, if the number is small, while it may satisfy the condition that "no specific entity (individual or corporation) has control over the decision-making process," it likely does not satisfy the criterion of "Is it practically controllable or difficult to control by regulatory authorities" On the other hand, if a licensed financial institution acts as the Sequencer, such needs for high decentralization are not present, so it is not a particular subject for discussion. Furthermore, while individuals and corporations can participate in the Lightning Network as part of the network that facilitates sending and receiving, in the case of current Rollup, the network for sending, receiving, and smart contracts is mostly composed of a single or small group of operators.

One of the critical aspects of Rollup is that users can retrieve their native tokens or other assets held on L2 back to L1 at their own discretion. While there is no clear standard on whether the 1st Layer's Native token becomes a "wrapped token" in a Public chain's 2nd Layer, the ability for a user to retrieve it to L1 without a Trusted third party is considered a crucial element. In Rollups, this execution is secured by the decentralization of the L1 (Decentralization of Ethereum L1 is outside the scope of this paper). This allows users on Rollup to hold the Native token in a non-custodial wallet. This characteristic is very important if the 2nd Layer is considered the interface with society.

In Bitcoin, the expressiveness of the script is limited, making it challenging for users to withdraw funds by their own will without a Trusted Third party (supported by a sufficiently large number of nodes) on Rollup-like architecture. The recent development of BitVM might increase the expressiveness of smart contracts on Bitcoin, but it is unclear how much, including user withdrawal capabilities, can be realized on decentraized way. Table 2 shows the characteristic comparison of Lightning Network and Rollups composed of a small number of BFT sequencers.

3.4 Discussion: Current State and Future Directions of Bitcoin Layer-2

As we have seen, the Pure Lightning Network in the Bitcoin 2nd Layer expands TPS and enables real-time transactions while largely preserving the properties

Table 2. The characteristics of the Lightning Network and rollups composed of a small number of sequencers with Byzantine fault tolerance

	decentralization	non-custodial easy UX	non-custodial wallet
Pure LN	Yes	Yes	No
rollups composed of a small number of BFT sequencers	No	Yes	Yes

of the 1st Layer. While there is an upper limit to the number of users, the current capacity is sufficient to handle present needs. However, the difficulty of the UX makes general adoption challenging, leading to high usage of the Custodial Lightning Network and the existence of intermediate solutions like LSP Mobile wallets. The fact that the majority of Lightning Network users use the Custodial Lightning Network is not necessarily an issue; as long as those who set up their own Lightning Network nodes can send and receive, it can be said that Decentralized innovation is being achieved. Since the network's nature is Permissionless, the creation of a Custodial Lightning Network on top of it is not inherently a problem. On the other hand, the number of Bitcoin 2nd Layer users is not exploding. This could be due to:

a) The current social demand for using Bitcoin for small-scale payments is not that large.
b) The technology is not yet easy enough for non-technical users.
c) A killer application that attracts a mass audience does not yet exist.

Regarding a), there is no technical solution. Regarding b), improvements in intermediate solutions or the development of new 2nd Layer forms may achieve this in the future. Various challenges are being pursued for c), but no definitive application has emerged yet.

In smart contract chains other than Bitcoin, tokenization finance and DeFi have gained attention as applications, with development being undertaken by large financial organizations. If Bitcoin succeeds as "an endeavor aimed at creating and disseminating Decentralized Money that anyone can hold and send by their own free will," finance will undoubtedly be a key application. In the report [7], while Bitcoin's capability as a monetary asset is highly rated, two future scenarios are presented for its use: one where it is used on other smart contract chains, and one where it is used on the Bitcoin protocol itself. If DeFi replaces the future of the financial industry, Decentralized Money should be used there. Conversely, the author believes that it cannot be considered a complete success if the majority of funds held in users' non-custodial wallets require trust in the conversion process, as is the case with Wrapped BTC.

Development is also progressing in the form of application-specific chain operators accepting Native Bitcoin from users. However, it is unclear what part will be conducted on a Public layer and what part will require business entities to be licensed, as we do not know how technology will advance, and which parts will achieve a level of Decentralization that is "difficult to control by regulatory

authorities." Meanwhile, it seems difficult for financial institutions to continue expanding financial services without KYC, considering business laws.

In this context, considering that financial services with KYC by large corporations may adopt native Bitcoin, while Bitcoin itself and highly decentralized applications succeed as an 'attempt to create and popularize decentralized money that anyone can hold and send by their own free will,' it seems essential to have numerous initiatives based on diverse architectures, especially given that the boundary between Layer 2 protocols and applications remains blurred(Fig. 4). Especially if the parts related to the Public layer are open source, it would contribute to the goal of "Bitcoin is an endeavor aimed at creating and disseminating Decentralized Money that anyone can hold and send by their own free will."

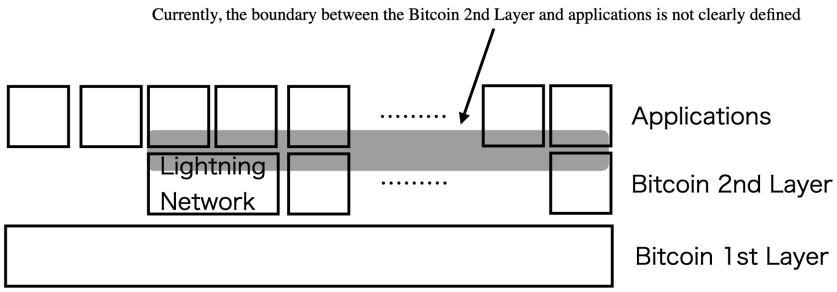


Fig. 4. Structure of 2nd Layer protocol and Applications

4 Conclusion

We have explained the difficulty of discussing the future of Bitcoin. This difficulty is a complex intertwining of factors: the inability to definitively state what Decentralization technology is meant to achieve, the uncertainty surrounding what will or will not be technically possible in the future, and the unpredictability of how future regulations will be applied. We took up the Bitcoin 2nd Layer, explaining the advantages and disadvantages of the Lightning Network. We used Ethereum Rollup as a comparison and analyzed it against the criteria discussed above. We offered the author's personal views on the future direction of the Bitcoin 2nd Layer. It is the author's hope that this paper helps mitigate the difficulty of discussions about Decentralization technology.

References

1. Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System https://bitcoin.org/bitcoin.pdf(2016)
2. Joseph Poon., Thaddeus Dryja: The Bitcoin Lightning Network:Scalable Off-Chain Instant Payments. https://lightning.network/lightning-network-paper.pdf(2016)
3. Shaolinfry.: BIP 148: Mandatory activation of segwit deployment,https://github.com/bitcoin/bips/blob/master/bip-0148.mediawiki
4. FATF: Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (2021)
5. BOLT: Basis of Lightning Technology (Lightning Network Specifications), https://github.com/lightning/bolts
6. The Practical Guide to Ethereum Rollups, https://hackernoon.com/the-practical-guide-to-ethereum-rollups
7. Chris Kuiper, Jack Meureuter, Bitcoin First: Why Investors Need to Consider Bitcoin Separately from Other Digital Assets